日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年１０月１２日
出願番号 Application Number:	特願２００４－２９８２４４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２９８２４４
出願人 Applicant(s):	日本電信電話株式会社

２００５年　９月１４日

特許庁長官
Commissioner,
Japan Patent Office

中嶋誠

【書類名】　特許願
【整理番号】　NTTH166071
【提出日】　平成16年10月12日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/66
H04L 12/56
【発明者】
【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
【氏名】　濱田　雅樹
【特許出願人】
【識別番号】　000004226
【氏名又は名称】　日本電信電話株式会社
【代理人】
【識別番号】　100089118
【弁理士】
【氏名又は名称】　酒井　宏明
【選任した代理人】
【識別番号】　100114306
【弁理士】
【氏名又は名称】　中辻　史郎
【手数料の表示】
【予納台帳番号】　036711
【納付金額】　16,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0310351

【書類名】特許請求の範囲
【請求項１】
サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、
前記監視装置は、
前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手段と、
前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手段と
を備え、
前記制限装置は、
前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限手段を備えたことを特徴とするサービス不能攻撃防御システム。
【請求項２】
前記監視装置は、前記通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成手段をさらに備え、前記防御要求情報送信手段は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記制限装置の前記パケット制限手段は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項１に記載のサービス不能攻撃防御システム。
【請求項３】
前記制限装置は、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを判断するシグネチャ判断手段をさらに備え、前記パケット制限手段は、前記シグネチャ判断手段によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項２に記載のサービス不能攻撃防御システム。
【請求項４】
前記制限装置は、前記シグネチャに該当するパケットの特徴や量に関するレポートを生成するレポート生成手段と、前記レポートを前記監視装置に送信するレポート送信手段とをさらに備え、前記シグネチャ生成手段は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手段は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手段は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項２または３に記載のサービス不能攻撃防御システム。
【請求項５】
前記制限装置は、前記防御要求情報を前記ＩＳＰ網に設けられた他の前記制限装置に転送する転送手段をさらに備え、前記転送手段は、前記レポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば前記防御要求情報を他の前記制限装置に転送することを特徴とする請求項４に記載のサービス不能攻撃防御システム。
【請求項６】
前記制限装置は、前記シグネチャ判断手段の判断結果を前記監視装置に送信する判断結果送信手段をさらに備え、前記監視装置の前記シグネチャ生成手段は、前記判断結果が前記シグネチャは適正でないことを表す場合に、該判断結果に基づいて前記通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することを特徴とする請求項３～５のいずれか一つに記載のサービス不能攻撃防御システム。
【請求項７】
サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不

能攻撃を防御するサービス不能攻撃防御方法であって、
前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知工程と、
前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信工程と
前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限工程と
を含んだことを特徴とするサービス不能攻撃防御方法。
【請求項８】
前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成工程をさらに含み、前記防御要求情報送信工程は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項７に記載のサービス不能攻撃防御方法。
【請求項９】
前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断工程をさらに含み、前記パケット制限工程は、前記シグネチャ判断工程によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項８に記載のサービス不能攻撃防御方法。
【請求項１０】
前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成工程と、前記レポートを前記監視装置に送信するレポート送信工程とをさらに含み、前記シグネチャ生成工程は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信工程は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項８または９に記載のサービス不能攻撃防御方法。
【請求項１１】
サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、
前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手順と、
前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手順と
前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限手順と
をコンピュータに実行させることを特徴とするサービス不能攻撃防御プログラム。
【請求項１２】
前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成手順をさらに含み、前記防御要求情報送信手順は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項１１に記載のサービス不能攻撃防御プログラム。
【請求項１３】
前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断手順をさらに含み、前記パケット制限手順は、前記シグネチャ判断手順によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケット

を制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項１２に記載のサービス不能攻撃防御プログラム。

【請求項１４】

前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成手順と、前記レポートを前記監視装置に送信するレポート送信手順とをさらに含み、前記シグネチャ生成手順は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手順は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項１２または１３に記載のサービス不能攻撃防御プログラム。

【書類名】明細書
【発明の名称】サービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラム
【技術分野】
【０００１】
この発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して通信機器に送信されたパケットを監視する監視装置およびＩＳＰ網に設けられかかるＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関し、特に、通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関する。
【背景技術】
【０００２】
従来、ネットワークを介した攻撃としてサービス不能攻撃(分散型サービス不能攻撃を含む)が知られている。かかるサービス不能攻撃から通信機器を防御するサービス不能攻撃防御システムでは、攻撃対象となるサーバマシン（以下「通信機器」と言う）を、ＩＳＰ（Internet Service Provider） 網に設けられたエッジルータが防御することになる。具体的には、サービス不能攻撃の１つであるＳＹＮ　Ｆｌｏｏｄ攻撃から保護するため、攻撃対象となる通信機器を含むＬＡＮ（Local Area Network）と接続されているＩＳＰ網のエッジルータは、ＬＡＮの出口回線にて、かかる通信機器を送信先とするＳＹＮパケットのトラヒック量に対して閾値を設け、この閾値を超えた部分のＳＹＮパケットを廃棄していた（例えば、特許文献１参照）。
【０００３】
【特許文献１】特開２００４－１６６０２９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来のサービス不能攻撃防御システムにおいては、ＩＳＰ側で通信機器に送信されるパケットの内容を監視・判断し制御する必要があるが、攻撃かとうかは情報の解釈が必要であり受け取り手でないと判断できない場合が多いため、通信の秘密順守や本来業務の範囲を逸脱しないようにする必要性から、攻撃が予め自明な一部のケースを除きＩＳＰ側で実施するには限界があるといった課題があった。
【０００５】
本発明は、上述した従来技術による問題点を解消するためになされたものであり、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
上述した課題を解決し、目的を達成するため、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記監視装置は、前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手段と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手段とを備え、前記制限装置は、前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限手段を備えたことを特徴とする。

【０００７】
この発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてＩＳＰ網を介して前記通信機器に送信されるパケットを制限することとしたので、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。
【０００８】
また、本発明は、上記発明において、前記監視装置は、前記通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成手段をさらに備え、前記防御要求情報送信手段は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記制限装置の前記パケット制限手段は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。
【０００９】
この発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。
【００１０】
また、本発明は、上記発明において、前記制限装置は、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを判断するシグネチャ判断手段をさらに備え、前記パケット制限手段は、前記シグネチャ判断手段によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする。
【００１１】
この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのパケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、パケットの制限が行われないため、他のＬＡＮに送信されるパケット等のような監視装置側で制限を要求してはならないパケットが制限装置によって制限されることを防止することができる。
【００１２】
また、本発明は、上記発明において、前記制限装置は、前記シグネチャに該当するパケットの特徴や量に関するレポートを生成するレポート生成手段と、前記レポートを前記監視装置に送信するレポート送信手段とをさらに備え、前記シグネチャ生成手段は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手段は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手段は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。
【００１３】
この発明によれば、制限装置がシグネチャに該当するパケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのパケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるパケットを制限し、その後にレポートに基づいて攻撃するパケットを特定して通信機器に対する攻撃を行わないパケットの制限を解除することができる。
【００１４】
また、本発明は、上記発明において、前記制限装置は、前記防御要求情報を前記ＩＳＰ

網に設けられた他の前記制限装置に転送する転送手段をさらに備え、前記転送手段は、前記レポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば前記防御要求情報を他の前記制限装置に転送することを特徴とする。

【００１５】

この発明によれば、制限装置がレポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば防御要求情報を他の制限装置に転送することとしたので、監視装置がかかるレポートに基づいて本来制限すべきでないパケットの通過制限解除を制限装置に依頼することにより、制限装置が行う通過制限をより適正化することができる。

【００１６】

また、本発明は、上記発明において、前記制限装置は、前記シグネチャ判断手段の判断結果を前記監視装置に送信する判断結果送信手段をさらに備え、前記監視装置の前記シグネチャ生成手段は、前記判断結果が前記シグネチャは適正でないことを表す場合に、該判断結果に基づいて前記通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することを特徴とする。

【００１７】

この発明によれば、制限装置がシグネチャ判断の判断結果を監視装置に送信し、監視装置は、受け取った判断結果がシグネチャは適正でないことを表す場合に、この判断結果に基づいて通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することとしたので、制限装置が不適正な通過制限を実行することを防止することができる。

【００１８】

また、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知工程と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信工程と前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限工程とを含んだことを特徴とする。

【００１９】

この発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてＩＳＰ網を介して前記通信機器に送信されるパケットを制限することとしたので、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００２０】

また、本発明は、上記発明において、前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成工程をさらに含み、前記防御要求情報送信工程は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【００２１】

この発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００２２】

また、本発明は、上記発明において、前記シグネチャを含む前記防御要求情報が適正な

ものであるか否かを前記制限装置が判断するシグネチャ判断工程をさらに含み、前記パケット制限工程は、前記シグネチャ判断工程によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする。

【００２３】

この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのパケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、パケットの制限が行われないため、他のＬＡＮに送信されるパケット等のような監視装置側で制限を要求してはならないパケットが制限装置によって制限されることを防止することができる。

【００２４】

また、本発明は、上記発明において、前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成工程と、前記レポートを前記監視装置に送信するレポート送信工程とをさらに含み、前記シグネチャ生成工程は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信工程は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【００２５】

この発明によれば、制限装置がシグネチャに該当するパケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのパケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるパケットを制限し、その後にレポートに基づいて攻撃するパケットを特定して通信機器に対する攻撃を行わないパケットの制限を解除することができる。

【００２６】

また、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたＬＡＮに設けられＩＳＰ網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ＩＳＰ網に設けられ前記ＬＡＮに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手順と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手順と前記防御要求情報に基づいて前記ＩＳＰ網を介して前記通信機器に送信されるパケットを制限するパケット制限手順とをコンピュータに実行させることを特徴とする。

【００２７】

この発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてＩＳＰ網を介して前記通信機器に送信されるパケットを制限することとしたので、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００２８】

また、本発明は、上記発明において、前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成手順をさらに含み、前記防御要求情報送信手順は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【００２９】

この発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグ

ネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００３０】

また、本発明は、上記発明において、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断手順をさらに含み、前記パケット制限手順は、前記シグネチャ判断手順によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする。

【００３１】

この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのパケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、パケットの制限が行われないため、他のＬＡＮに送信されるパケット等のような監視装置側で制限を要求してはならないパケットが制限装置によって制限されることを防止することができる。

【００３２】

また、本発明は、上記発明において、前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成手順と、前記レポートを前記監視装置に送信するレポート送信手順とをさらに含み、前記シグネチャ生成手順は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手順は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【００３３】

この発明によれば、制限装置がシグネチャに該当するパケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのパケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるパケットを制限し、その後にレポートに基づいて攻撃するパケットを特定して通信機器に対する攻撃を行わないパケットの制限を解除することができる。

【発明の効果】

【００３４】

本発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてＩＳＰ網を介して前記通信機器に送信されるパケットを制限することとしたので、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００３５】

また、本発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【００３６】

また、本発明によれば、制限装置がシグネチャを含む防護要求情報が適正なものである

が否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのパケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、パケットの制限が行われないため、他のＬＡＮに送信されるパケット等のような監視装置側で制限を要求してはならないパケットが制限装置によって制限されることを防止することができる。

【００３７】

また、本発明によれば、制限装置がシグネチャに該当するパケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのパケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるパケットを制限し、その後にレポートに基づいて攻撃するパケットを特定して通信機器に対する攻撃を行わないパケットの制限を解除することができる。

【００３８】

また、本発明によれば、制限装置がレポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば防御要求情報を他の制限装置に転送することとしたので、監視装置がかかるレポートに基づいて本来制限すべきでないパケットの通過制限解除を制限装置に依頼することにより、制限装置が行う通過制限をより適正化することができる。

【００３９】

また、本発明によれば、制限装置がシグネチャ判断の判断結果を監視装置に送信し、監視装置は、受け取った判断結果がシグネチャは適正でないことを表す場合に、この判断結果に基づいて通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することとしたので、制限装置が不適正な通過制限を実行することを防止することができる。

【発明を実施するための最良の形態】

【００４０】

以下に添付図面を参照して、この発明に係るサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムの好適な実施の形態を詳細に説明する。

【実施例】

【００４１】

図１は、本実施例に係るサービス不能攻撃防御システム１の構成を示すブロック図である。同図に示すサービス不能防御システム１は、通信機器３へのサービス不能攻撃を監視装置５および制限装置６で防御するシステムである。具体的には、ＬＡＮ２上の監視装置５が通信機器３へのサービス不能攻撃を検知したならば（図１のステップ１）、攻撃の特徴を表すシグネチャを生成してかかるシグネチャを含む防御要求情報をＩＳＰ網４上の制限装置６に送信する（図１のステップ２）。そして、防御要求情報を受信した制御装置６は、防御要求情報に含まれるシグネチャに基づいてサービス不能攻撃を行うパケットの通過を制限することにより防御を実行する（図１のステップ３）こととしている。

【００４２】

従来、ＩＳＰ網４上の制限装置６では、攻撃と思われるパケットが通過した場合であっても、攻撃かどうかはパケットに含まれる情報の解釈が必要であり受け取り手でないと判断できない場合が多いため、ＩＳＰ網４を運営するＩＳＰは、通信の秘密順守や本来業務の範囲を逸脱しないようにする必要性から、攻撃が予め自明な一部のケースを除き、かかるパケットの制限を行うことができないという問題があった。本実施例では、パケットに含まれる情報の解釈をＬＡＮ２上の監視装置５が行い、監視装置５が検出した攻撃パケットの通過制限をＩＳＰ網４上の制限装置６が行うこととしている。このため、本実施例によれば、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲内で通信装置３を攻撃するパケットを効果的に制限することができる。

【００４３】
また、かかる制限装置６は、監視装置５が検出した攻撃パケットの通過制限を行った場合に、この通過制限の内容を表すレポートを監視装置５に送信することとしている。このため、監視装置５がかかるレポートに基づいて本来制限すべきでないパケットの通過制限解除を制限装置６に依頼することにより、制限装置６が行う通過制限をより適正化することができる。
【００４４】
さらに、かかる制限装置６は、監視装置５からパケットの通過制限を依頼された場合に、依頼内容が適正であるものについてのみ通過制限を実行することとしている。このため、制限装置６が不適正な通過制限を実行することを防止することができる。
【００４５】
次に、このサービス不能攻撃防御システム１のシステム構成について説明する。図１に示すように、このサービス不能攻撃防御システム１は、中小企業内に設けられたＬＡＮ２に設けられ、ＬＡＮ２に接続された少なくとも１つの通信機器３に基幹回線網等のＩＳＰ網４を介して送信されたパケットを監視する監視装置５と、ＬＡＮ２をＩＳＰ網４に接続する制限装置６とを備えている。なお、図１に示したサービス不能攻撃防御システム１の構成は一例を示すものであり、本発明のサービス不能攻撃防御システムは、複数の制限装置６を備えてもよく、各制限装置６に対して複数の監視装置５をそれぞれ備えてもよい。
【００４６】
監視装置５は、ＬＡＮ２を構成するルータによって構成されている。なお、監視装置５は、ＬＡＮ２に設けられたファイアウォール等によって構成してもよい。
【００４７】
図２は、図１に示した監視装置５の構成を示すブロック図である。監視装置５は、通信機器３に送信されるパケットによる攻撃を検知する攻撃検知部１０と、攻撃に対する防御の要求を表す防御要求情報を制限装置６に送信する防御要求情報送信部１１と、通信機器３に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成部１２と、制限装置６およびＬＡＮ２に設けられた各装置とそれぞれ通信を行うための通信インタフェイス１３、１４と、パケットをルーティングするためのスイッチ１５とを備えている。
【００４８】
攻撃検知部１０は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図３は、攻撃検知条件の一例を示す図である。図３において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる３組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。
【００４９】
例えば、１番目の検知条件は、宛先のアドレス情報が192.168.1.1であり（Dst=192.168.1.1/32）、トランスポート層のプロトコルがＴＣＰ（Transmission Control Protocol）であり（Protocol=TCP）、ＴＣＰポート番号が８０である（Port=80）パケットが検知対象となり、この検知対象のパケットの伝送レートが５００kbpsを超えた状態が１０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
【００５０】
同様に、２番目の検知条件は、宛先のアドレス情報が192.168.1.2であり（Dst=192.168.1.2/32）、トランスポート層のプロトコルがＵＤＰ（User datagram protocol）である（Protocol=UDP）パケットが検知対象となり、この検知対象のパケットの伝送レートが３００kbpsを超えた状態が１０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。
【００５１】
また、３番目の検知条件は、宛先のアドレス情報が192.168.1.0～192.168.1.255の範囲

内である（dst=192.168.1.0/24）パケットが検知対象となり、この検知対象のパケットの伝送レートが１Mbpsを超えた状態が２０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【００５２】

このように、検知対象のパケットによる攻撃が攻撃検知部１０によって検知されると、シグネチャ生成部１２は、検知対象のパケットの特徴を表すシグネチャを生成するようになっている。例えば、図３における攻撃検知条件の１番目の検知条件に合う攻撃が検知された場合には、シグネチャ生成部１２は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがＴＣＰであり、ＴＣＰポート番号が８０であるパケットを示すシグネチャを生成する。なお、シグネチャは、対象となるパケットに対する制御方法としてシェーピングやフィルタリング等の処理の指定や、この処理に関するパラメータ等を含むようにしてもよい。

【００５３】

防御要求情報送信部１１は、シグネチャ生成部１２によって生成されたシグネチャを含み、攻撃に対する防御の要求を表す防御要求情報を制限装置６に送信する処理部である。なお、防御要求情報送信部１１は、パケットが送受信される伝送路７とは異なる通信経路で防御要求情報を送信するようにしてもよい。

【００５４】

図１に示した制限装置６は、ＬＡＮ２をＩＳＰ網４に接続するエッジルータによって構成されている。なお、ここでは説明の便宜上制限装置６の構成を説明するが、他の制限装置８～９についても制限装置６と同様に構成されている。

【００５５】

図４は、図１に示した制限装置６の構成を示すブロック図である。この制限装置６は、防御要求情報に基づいてＩＳＰ網４を介して通信機器３に送信されるパケットを制限するパケット制限部２０と、防御要求情報を他のパケット制限装置に転送する防御要求情報転送部２１と、シグネチャを含む防護要求情報が適正なものであるか否かを判断するシグネチャ判断部２２と、シグネチャ判断部２２による判断結果を監視装置５に送信する判断結果送信部２３と、シグネチャに当てはまるパケットの特徴や量に関するレポートを生成するレポート生成部２４と、レポートを監視装置５に送信するレポート送信部２５と、監視装置５およびＩＳＰ網４に設けられた各装置とそれぞれ通信を行うための通信インタフェイス２６、２７と、パケットをルーティングするためのスイッチ２８とを備えている。

【００５６】

シグネチャ判断部２２は、監視装置５から送信された防御要求情報に含まれるシグネチャを含む防護要求情報が適正なものであるか否かを判断する処理部である。ここで、シグネチャ判断部２２は、他のＬＡＮに送信されるパケット等のような監視装置５側で制限を要求してはならないパケットが制限装置６によって制限されることを防止する。

【００５７】

パケット制限部２０は、シグネチャ判断部２２によってシグネチャを含む防護要求情報が適正なものであると判断された場合には、監視装置５から送信された防御要求情報に含まれるシグネチャに該当するパケットを制限する処理部である。

【００５８】

シグネチャ判断部２２による判断結果は、判断結果送信部２３によって監視装置５に送信される。なお、判断結果送信部２３は、パケットが送受信される伝送路７とは異なる通信経路で判断結果を送信するようにしてもよい。

【００５９】

ここで、監視装置５のシグネチャ生成部１２は、送信された判断結果に応じてシグネチャを再生成するようにしてもよい。例えば、防御要求情報送信部１１によって送信された防御要求情報が、あるネットワークアドレスから送信されたパケットの制限を要求し、この要求が適正なものではないとシグネチャ判断部２２によって判断された判断結果が判断結果送信部２３によって送信された場合には、シグネチャ生成部１２は、攻撃検知部１０

を介して各トラフィックの量を測定し、上述したネットワークアドレスが示すネットワーク内でトラフィックが高いホストから送信されたパケットを制限するようシグネチャを再生成する。

【００６０】

なお、シグネチャ生成部１２によるシグネチャの再生成は、判断結果送信部２３によって送信された判断結果を見たＬＡＮ２の管理者によるオペレーションによって行われるようにしてもよい。

【００６１】

レポート生成部２４は、監視装置５から送信された防御要求情報に含まれるシグネチャに該当するパケットの特徴や量に関するレポートを生成する処理部である。例えば、レポート生成部２４は、シグネチャに該当するパケットのヘッダ部に含まれる送信元のアドレス情報と、当該パケットの伝送量とを対応させるテーブルを含むレポートを生成する。

【００６２】

レポート生成部２４によって生成されたレポートは、レポート送信部２５によって監視装置５に送信される。なお、レポート送信部２５は、パケットが送受信される伝送路７とは異なる通信経路でレポートを送信するようにしてもよい。

【００６３】

ここで、監視装置５のシグネチャ生成部１２は、送信されたレポートに応じてシグネチャを再生成する。なお、このシグネチャ生成部１２によるシグネチャの再生成は、レポート送信部２５によって送信されたレポートを見たＬＡＮ２の管理者によるオペレーションによって行われるようにしてもよい。

【００６４】

監視装置５の防御要求情報送信部１１は、シグネチャ生成部１２によって再生成されたシグネチャを含む防御要求情報を制限装置６に再送信し、制限装置６のパケット制限部２０は、シグネチャ判断部２２によってシグネチャを含む防護要求情報が適正なものであると判断された場合には、監視装置５から再送信された防御要求情報に含まれるシグネチャに該当するパケットを制限する。

【００６５】

このように、かかるレポートに基づいてシグネチャを再生成することによって、通信機器３に対する攻撃を行っていないパケットや、通信機器３に対する攻撃を現に行っているパケット等を特定し、制限対象となるパケットを絞りこんだ制限を課していくことができる。したがって、通信機器３に対する攻撃を行っておらず本来制限すべきでないパケットの制限を解除することができる。

【００６６】

防御要求情報転送部２１は、監視装置５から送信された防御要求情報を制限装置６と同様に構成された他のパケット制限装置（例えば、図１に示したパケット制限装置８、９）に転送するか否かをレポート生成部２４によって生成されたレポートに基づいて判断し、防御要求情報を他のパケット制限装置に転送すると判断した場合には、防御要求情報を他のパケット制限装置に転送する。

【００６７】

以上のように構成されたサービス不能攻撃防御システム１について、図５～図７を用いてその動作を説明する。図５は、図２に示した監視装置５の攻撃検知動作を示すフローチャートである。

【００６８】

まず、通信機器３に送信されるパケットによる攻撃が攻撃検知部１０によって攻撃検知条件に基づいて検知されると（ステップＳ１）、攻撃が検知されたパケットの特徴を表すシグネチャがシグネチャ生成部１２によって生成され（ステップＳ２）、生成されたシグネチャを含む防御要求情報が防御要求情報送信部１１によって制限装置６に送信される（ステップＳ３）。

【００６９】

ここで、防御要求情報の送信に応じて制限装置６から送信されたシグネチャを含む防護要求情報が適正なものであるか否かの判断結果が通信インタフェイス１３に受信され（ステップＳ４）、この判断結果にシグネチャが適正なものではないことが示されている場合（ステップＳ５）には、この判断結果に基づいてシグネチャ生成部１２によってシグネチャが再生成され（ステップＳ２）、再生成されたシグネチャを含む防御要求情報が防御要求情報送信部１１によって制限装置６に再送信される（ステップＳ３）。

【００７０】

また、制限装置６によって送信されたレポートが通信インタフェイス１３に受信された場合（ステップＳ６）には、受信されたレポートに基づいてシグネチャを再生成するか否かがシグネチャ生成部１２によって判断され（ステップＳ７）、シグネチャを再生成すると判断された場合には、レポートに基づいてシグネチャ生成部１２によってシグネチャが再生成され（ステップＳ２）、再生成されたシグネチャを含む防御要求情報が防御要求情報送信部１１によって制限装置６に再送信される（ステップＳ３）。

【００７１】

図６は、図４に示した制限装置６の防御要求情報受信動作を示すフローチャートである。監視装置５から送信された防御要求情報が通信インタフェイス２６に受信されると（ステップＳ１０）、受信された防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるか否かがシグネチャ判断部２２によって判断される（ステップＳ１１）。

【００７２】

防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるとシグネチャ判断部２２によって判断された場合には、シグネチャがパケット制限部２０に設定される（ステップＳ１２）。また、防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるか否かのシグネチャ判断部２２による判断の結果は、判断結果送信部２３によって監視装置５に送信される（ステップＳ１３）。

【００７３】

図７は、図４に示した制限装置６のレポート送信動作を示すフローチャートである。パケット制限部２０にシグネチャが設定されている場合（ステップＳ２０）には、監視装置５から送信された防御要求情報に含まれるシグネチャに該当するパケットの特徴や量に関するレポートがレポート生成部２４によって生成され（ステップＳ２１）、生成されたレポートがレポート送信部２５によって監視装置５に送信される（ステップＳ２２）。

【００７４】

また、レポート生成部２４によって生成されたレポートに基づいて、通信インタフェイス２６に受信された防御要求情報をパケット制限装置８、９等の他のパケット制限装置に転送するか否かが防御要求情報転送部２１によって判断され（ステップＳ２３）、防御要求情報を他のパケット制限装置に転送すると判断された場合には、防御要求情報が防御要求情報転送部２１によって他のパケット制限装置に転送される（ステップＳ２４）。

【００７５】

このように、レポート送信部２５によって送信されたレポートに基づいて攻撃の終了が監視装置５で検知され、防御要求情報送信部１１によって所定の防御要求情報が制限装置６に送信されることによってパケット制限部２０によるパケットの制限が解除される。

【００７６】

上述してきたように、サービス不能攻撃防御システム１によれば、ＬＡＮ２側で通信機器３に対する攻撃が検知され、検知された攻撃の防御要求に基づいてＩＳＰ網４側の制限装置６で通信機器３に送信されるパケットが制限されるため、ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器３を防御することができる。

【００７７】

なお、上記実施例に示した監視装置および制限装置は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、監視装置のコンピュータのＲＯＭ（Read Only Memory）等に通信機器を攻撃するパケットを検知するルーチン、制限装置

に対して防護要求情報を送信するルーチンを含むプログラムを記憶し、また、制限装置のコンピュータのＲＯＭ等に通信機器へ攻撃を行うパケットの通過を防護要求情報に基づいて制限するルーチンを含むプログラムを記憶しておき、各装置がこれらのプログラムをＣＰＵにロードして実行することにより、本発明に係る監視装置および制限装置を形成することができる。

【産業上の利用可能性】

【００７８】

以上のように、本発明にかかるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムは、サービス不能攻撃から通信機器を防御する場合に適している。

【図面の簡単な説明】

【００７９】

【図１】本実施例に係るサービス不能攻撃防御システムの構成を示すブロック図である。

【図２】図１に示した監視装置の構成を示すブロック図である。

【図３】本実施例に係る攻撃検知条件の一例を示す図である。

【図４】図１に示した制限装置の構成を示すブロック図である。

【図５】図２に示した監視装置の攻撃検知動作を示すフローチャートである。

【図６】図４に示した制限装置の防御要求情報受信動作を示すフローチャートである。

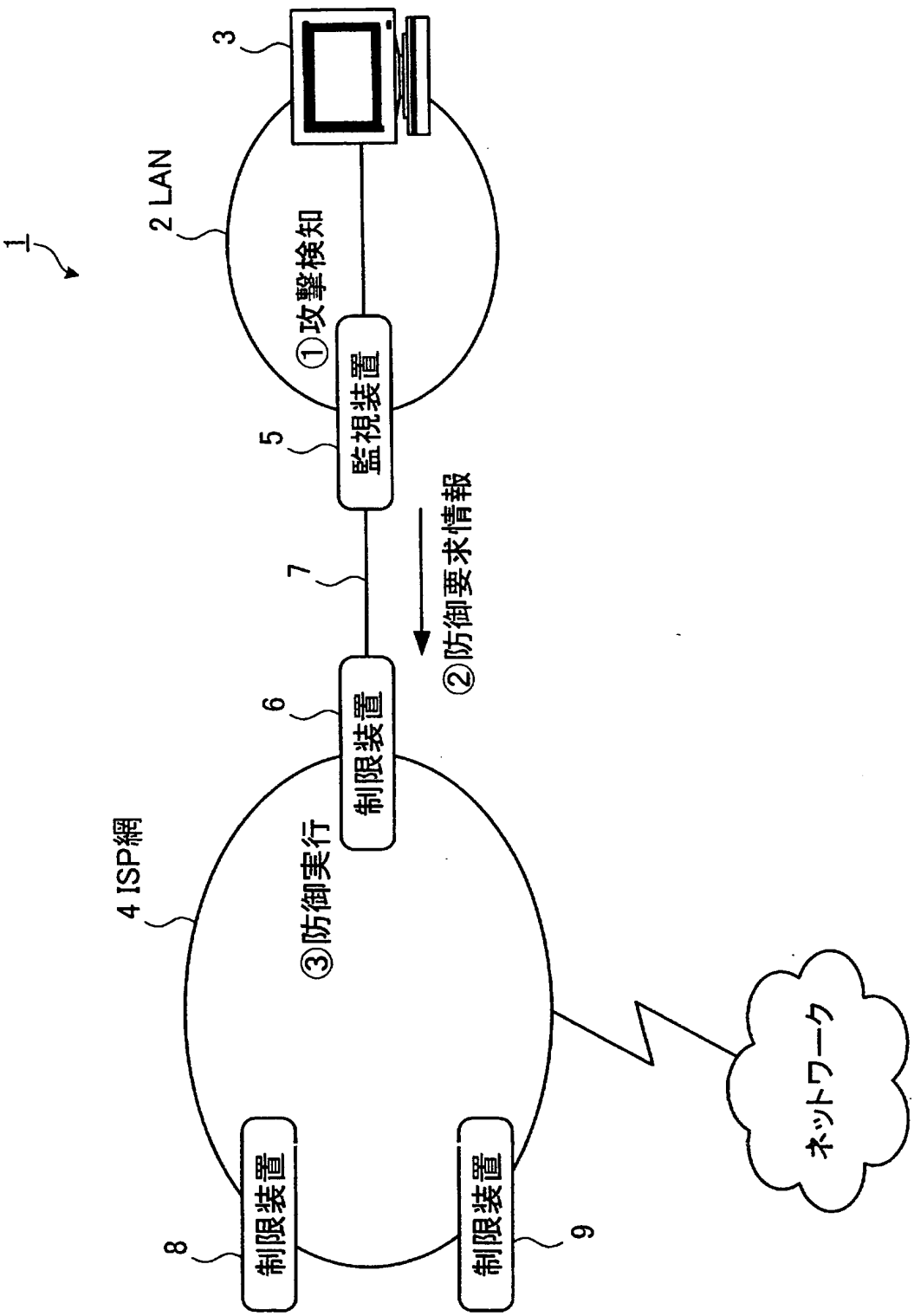
【図７】図４に示した制限装置のレポート送信動作を示すフローチャートである。

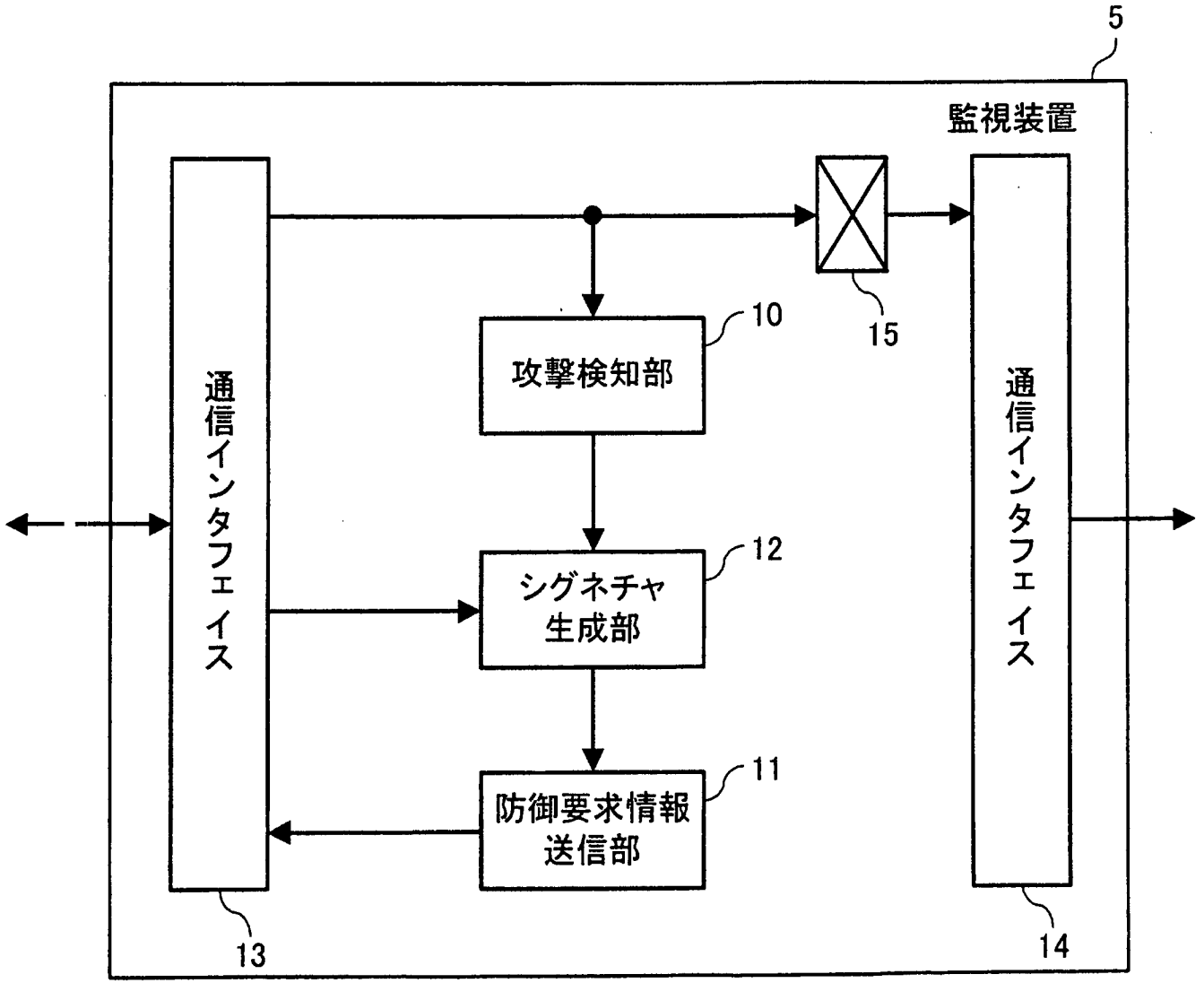
【符号の説明】

【００８０】

１　サービス不能攻撃防御システム
２　ＬＡＮ
３　通信機器
４　ＩＳＰ網
５　パケット監視装置
６、８、９　パケット制限装置
７　伝送路
１０　攻撃検知部
１１　防御要求情報送信部
１２　シグネチャ生成部
１３、１４、２６、２７　通信インタフェイス
１５、２８　スイッチ
２０　パケット制限部
２１　防御要求情報転送部
２２　シグネチャ判断部
２３　判断結果送信部
２４　レポート生成部
２５　レポート送信部

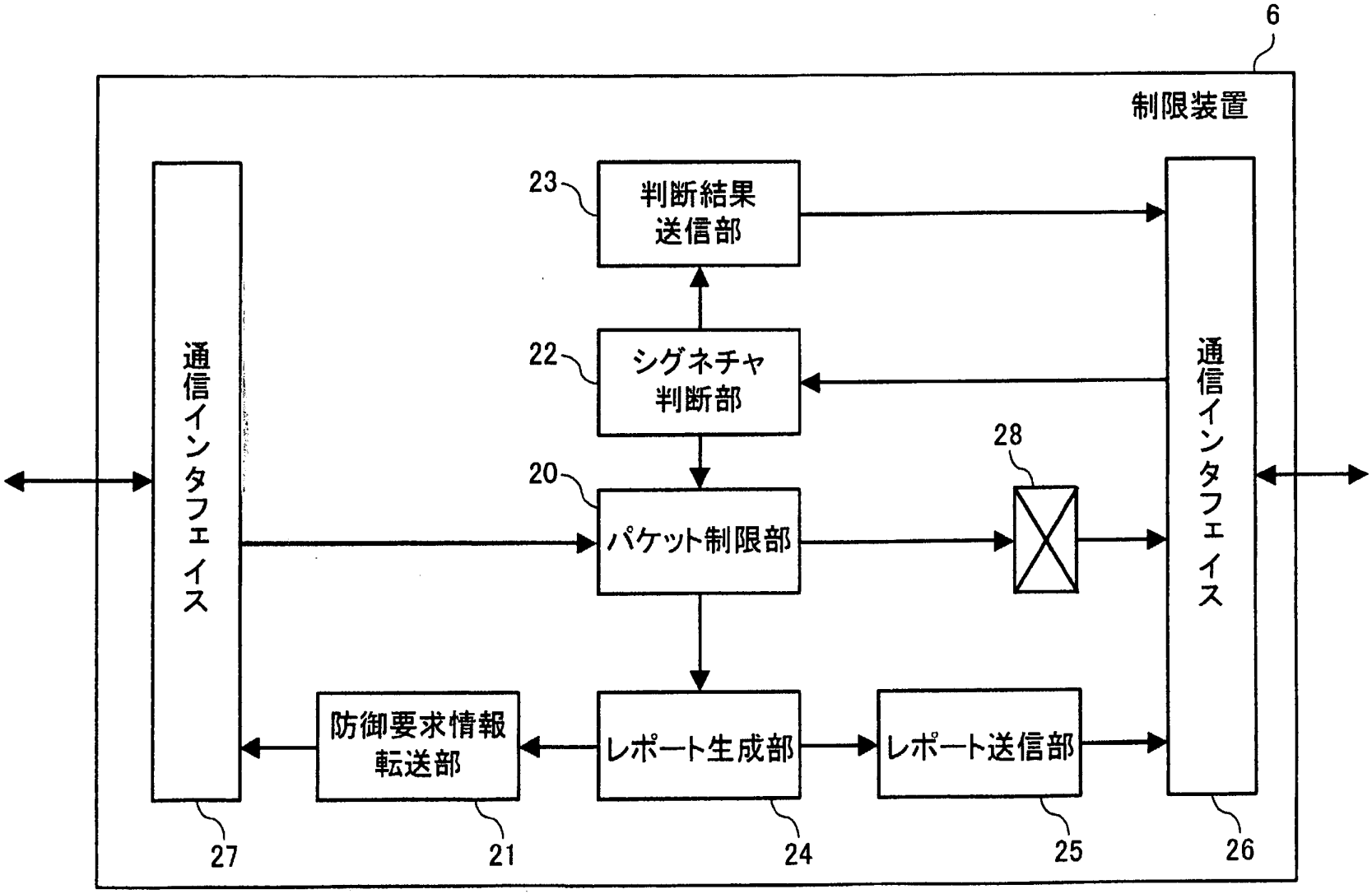
【書類名】図面
【図１】

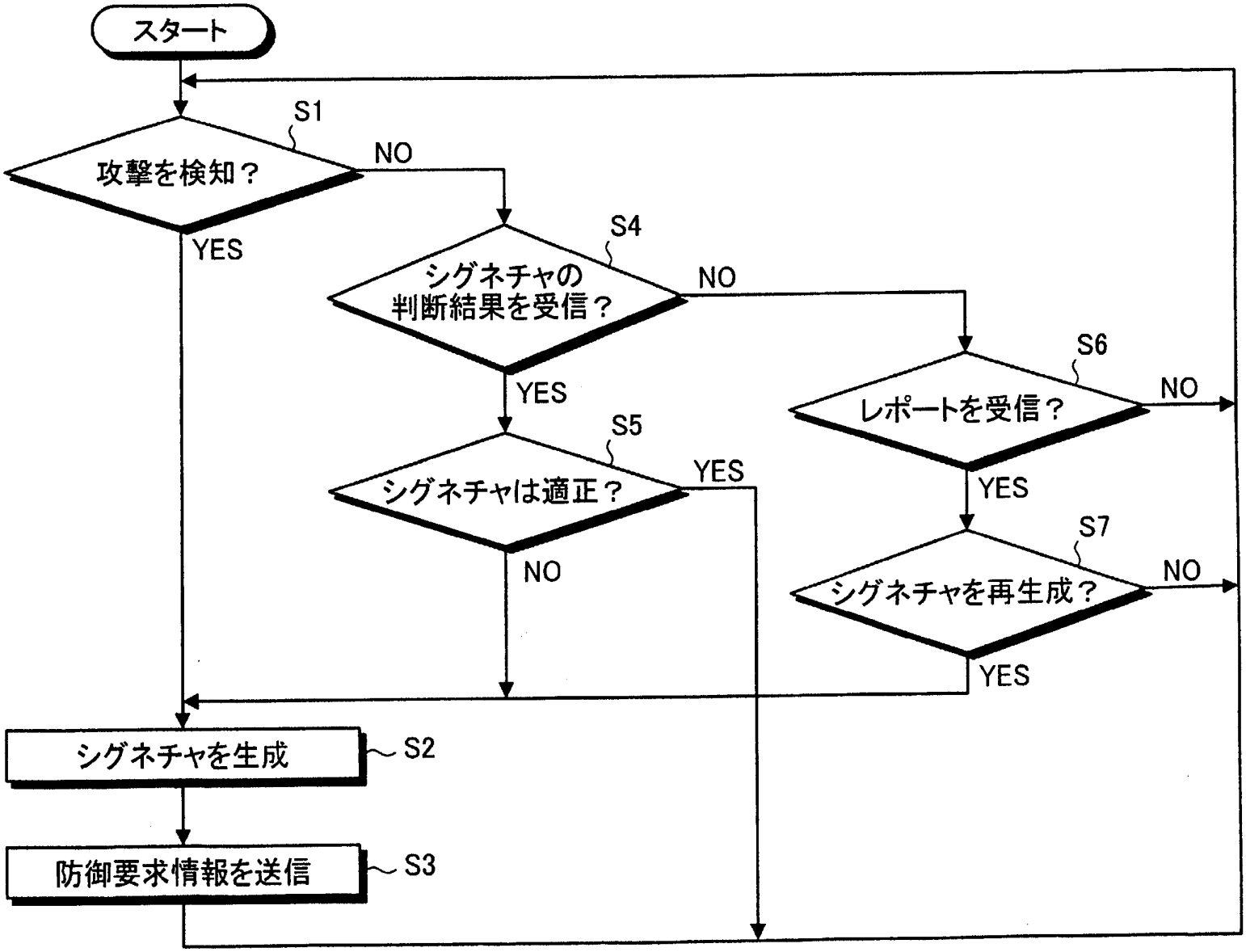

1
2 LAN
3
①攻撃検知
監視装置
5
7
②防御要求情報
6
制限装置
4 ISP網
③防御実行
制限装置
8
制限装置
9
ネットワーク

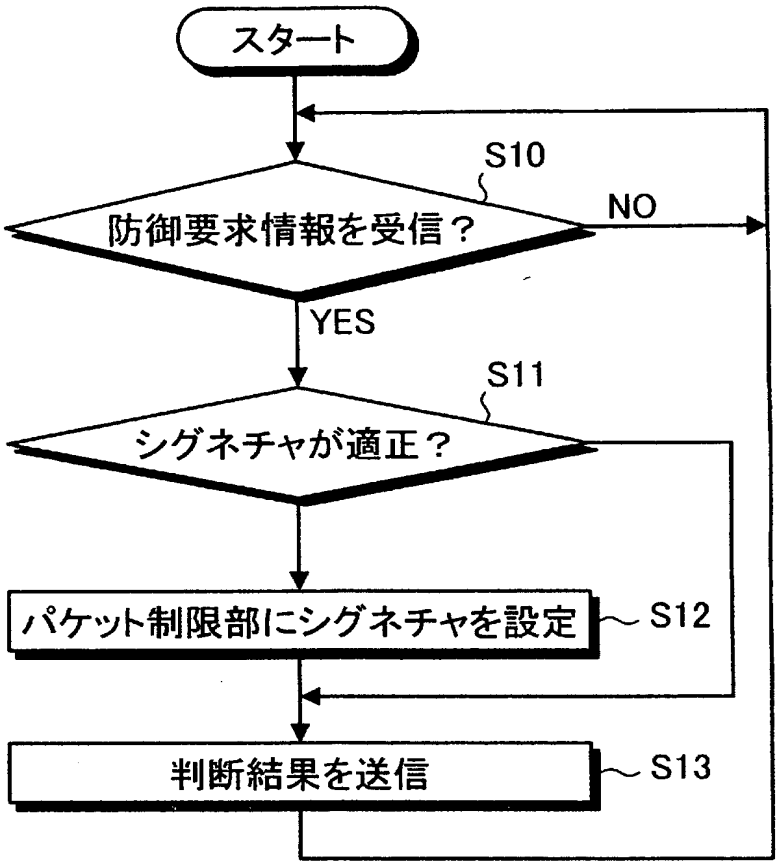

5
監視装置
通信インタフェイス
攻撃検知部
10
15
シグネチャ生成部
12
防御要求情報送信部
11
通信インタフェイス
13
14

【図3】

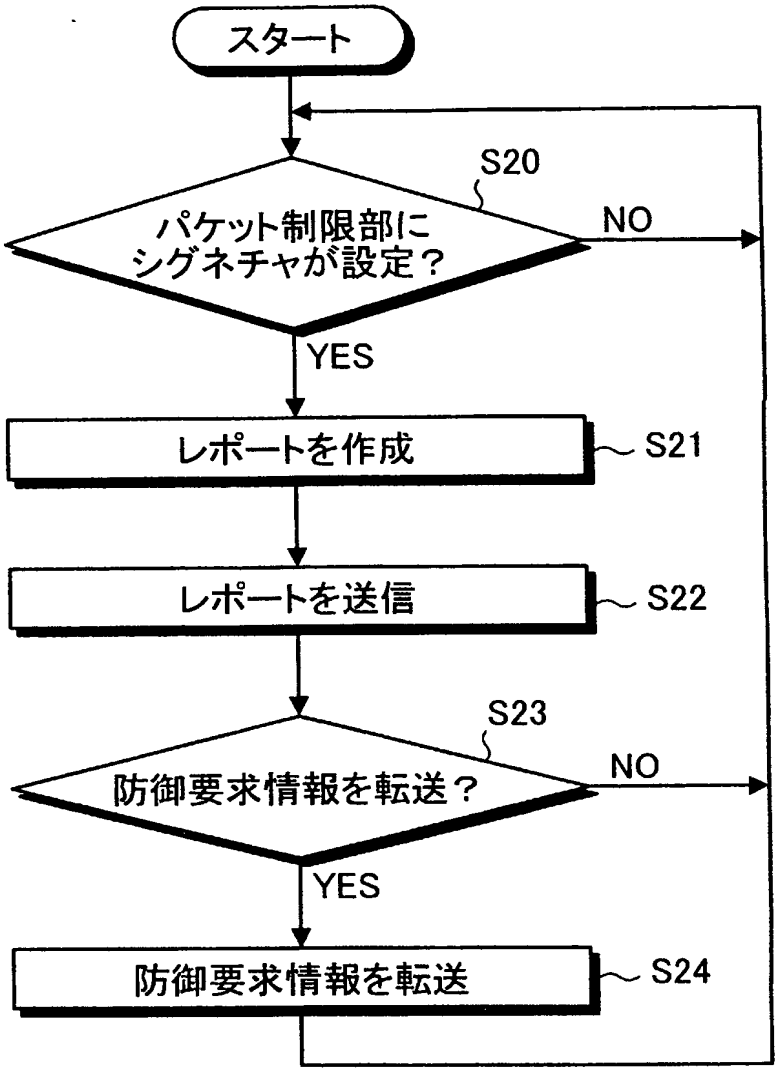
	検知属性	検知閾値	検出時間
1	{Dst=192.168.1.1/32, Protocol=TCP, Port=80}	500kbps	10秒
2	{Dst=192.168.1.2/32, Protocol=UDP}	300kbps	10秒
3	{Dst=192.168.1.0/24}	1Mbps	20秒


6
制限装置
通信インタフェイス
23
判断結果送信部
22
シグネチャ判断部
20
パケット制限部
28
通信インタフェイス
防御要求情報転送部
レポート生成部
レポート送信部
27
21
24
25
26


スタート
S1
攻撃を検知？
NO
YES
S4
シグネチャの
判断結果を受信？
NO
YES
S5
シグネチャは適正？
YES
NO
S6
レポートを受信？
NO
YES
S7
シグネチャを再生成？
NO
YES
シグネチャを生成
S2
防御要求情報を送信
S3


スタート
S10
防御要求情報を受信？
NO
YES
S11
シグネチャが適正？
パケット制限部にシグネチャを設定
S12
判断結果を送信
S13

【図７】


スタート
S20
パケット制限部にシグネチャが設定？
NO
YES
レポートを作成
S21
レポートを送信
S22
S23
防御要求情報を転送？
NO
YES
防御要求情報を転送
S24

【書類名】要約書
【要約】
【課題】ＩＳＰが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システムを提供することを課題とする。
【解決手段】ＬＡＮ２に設けられ、ＬＡＮ２に接続された少なくとも１つの通信機器３にＩＳＰ網４を介して送信されたパケットを監視する監視装置５と、ＩＳＰ網４内に設けられ、ＬＡＮ２に向かうパケットを制限する制限装置６とを備え、監視装置５は、通信機器３に対するパケットによる攻撃を検知し、検知した攻撃に対する防御の要求を表す防御要求情報を制限装置６に送信し、制限装置６は、防御要求情報に基づいてＩＳＰ網４を介して通信機器３に送信されるパケットを制限する。
【選択図】　図１

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/015155

International filing date: 19 August 2005 (19.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298244
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 29 September 2005 (29.09.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse